Claims

WE CLAIM:

1. A method for processing a permission set associated with a code assembly received from a resource location to control execution of the code assembly, the method comprising:

receiving the permission set including at least one permission associated with the code assembly;

receiving a permission request set in association with the code assembly; and

filtering the permission set based on the permission request set to control execution of the code assembly.

2. The method of claim 1 wherein the filtering operation comprises:

generating a permission grant set from a subset of the permission set, the subset specified by the permission request set.

3. The method of claim 1 wherein the filtering operation comprises:

computing a logical set operation on the permission set and the permission request set to generate a permission grant set.

4. The method of claim 1 wherein the permission request set specifies a minimum permission condition and the filtering operation comprises:

preventing loading of the code assembly, if the permission set fails to satisfy the minimum permission condition.

5. The method of claim 1 wherein the permission request set specifies a minimum permission condition and the filtering operation comprises:

preventing execution of the code assembly, if the permission set fails to satisfy the minimum permission condition.

6. The method of claim 1 further comprising:

defining a code group collection based on a security policy specification, the code group collection including one or more code groups;

receiving evidence associated with the code assembly;

evaluating membership of the code assembly in the one or more code groups, based on the evidence; and

generating the permission set based on the membership of the code assembly in the one or more code groups.

7. The method of claim 1 wherein the permission request set specifies a plurality of typed permission request sets, each typed permission request set specifying a distinct type of permission preference requested in association with the code assembly.

8. The method of claim 1 wherein the permission request set specifies a minimum request set specifying a minimum set of permissions requested in association with the code assembly.

9. The method of claim 8 wherein the filtering operation comprises:

filtering the permission set based on the minimum request set to generate a permission grant set, such that the permission grant set includes a subset of the permission set.

10. The method of claim 8 further comprising:

preventing loading of the code assembly, if the minimum request set is not a subset of the permission set.

11. The method of claim 8 further comprising:

preventing execution of the code assembly, if the minimum request set is not a subset of the permission set.

12. The method of claim 1 wherein the permission request set specifies an optional request set specifying an optional set of permissions requested in association with the code assembly.

13. The method of claim 12 wherein the filtering operation comprises filtering the permission set based on the optional request set to generate a permission grant set; and further comprising:

executing a first level of code assembly functionality if the optional request set is a subset of the permission grant set; and

executing a second level of code assembly functionality if the optional request set is not a subset of the permission grant set.

14. The method of claim 1 wherein the permission request set specifies a refuse request set specifying a set of one or more permissions to be omitted from a permission grant set in associated with the code assembly.

15. The method of claim 14 wherein the filtering operation comprises:

omitting the set of one or more permissions specified by the refuse request set from the permission grant set.

16. The method of claim 1 wherein the permission request set includes an optional request set specifying an optional set of permissions requested in association with the code assembly and a minimum request set specifying a minimum set of permissions requested in association with the code assembly, and wherein the filtering operation comprises:

computing a union of the optional request set and minimum request set to provide a maximum request set; and

computing an intersection of the maximum request set and the permission set.

17. The method of claim 16 wherein the permission request set further specifies a refuse request set specifying a set of one or more permissions to be omitted from a permission grant set in associated with the code assembly, and wherein the filtering operation further comprises:

subtracting the set of one or more permissions specified in the refuse request set from the intersection of the maximum request set and the permission set.

18. The method of claim 1 wherein the operation of receiving a permission request set comprises:

receiving the permission request set and the code assembly in a single network communication.

19. The method of claim 1 wherein the operation of receiving a permission request set

comprises:

retrieving the permission request set in a network communication distinct from a network communication in which the code assembly is received.

20. A policy manager module for processing a permission set associated with a code assembly received from a resource location to control execution of the code assembly, the policy manager module comprising:

a filter receiving the permission set and a permission request set associated with the code assembly and filtering the permission set based on the permission request set to control execution of the code assembly.

21. The policy manager module of claim 20 further comprising:

a permission set generator receiving an evidence set and generating a permission set in association with the code assembly, based on the evidence set.

22. The policy manager module of claim 20 wherein the filter generates a permission grant set from a subset of the permission set specified by the permission request set.

23. The policy manager module of claim 20 wherein the filter computes a logical set operation on the permission set and the permission request set to generate a permission grant set.

24. The policy manager module of claim 20 wherein the filter prevents loading of the code assembly, if the permission set fails to satisfy the minimum permission condition.

25. The policy manager module of claim 20 wherein the filter prevents execution of the code assembly, if the permission set fails to satisfy the minimum permission condition.

26. The policy manager module of claim 20 wherein the permission request set specifies a plurality of typed permission request sets, each typed permission request set specifying a

distinct type of permission preference requested in association with the code assembly.

27. The policy manager module of claim 20 wherein the permission request set specifies a minimum request set specifying a minimum set of permissions requested in association with the code assembly.

28. The policy manager module of claim 20 wherein the permission request set specifies an optional request set specifying an optional set of permissions requested in association with the code assembly.

29. The policy manager module of claim 20 wherein the filter generates a permission grant set omitting one or more permissions specified in a refuse request set.

30. The policy manager module of claim 20 wherein the permission request set specifies an optional request set specifying an optional set of permissions requested in association with the code assembly and a minimum request set specifying a minimum set of permissions requested in association with the code assembly, and wherein the filtering operation comprises:

computing a union of the optional request set and minimum request set to provide an maximum request set; and

computing an intersection of the maximum request set and the permission set.

31. The policy manager module of claim 20 wherein the filter generates a permission grant set based on an optional request set, the permission grant set being associated with a first level of code assembly functionality if the optional request set is a subset of the permission grant set and being associated with a second level of code assembly functionality if the optional

request set is not a subset of the permission grant set.

32. The policy manager module of claim 20 further comprising:

a code group collection generator creating a code group collection based on a security policy specification, the code group collection including one or more code groups;

a membership evaluator determining membership of the code assembly in the one or more code groups, based on evidence associated with the code assembly; and

a permission set generator creating the permission set based on the membership of the code assembly in the one or more code groups.

33. A computer data signal embodied in a carrier wave by a computing system and encoding a computer program for executing a computer process processing a permission set associated with a code assembly received from a resource location to control execution of the code assembly, the computer process comprising:

receiving the permission set including at least one permission associated with the code assembly;

receiving a permission request set in association with the code assembly; and

filtering the permission set based on the permission request set to control execution of the code assembly.

34. A computer program storage medium readable by a computer system and encoding a computer program for executing a computer process processing a permission set associated with a code assembly received from a resource location, the computer process comprising:

receiving the permission set including at least one permission associated with the code assembly;

receiving a permission request set in association with the code assembly; and

filtering the permission set based on the permission request set to control execution of the code assembly.

35. A computer program product encoding a computer program for executing on a computer system a computer process processing a permission set associated with a code assembly received from a resource location to control execution of the code assembly, the computer process comprising:

defining a code group collection based on a security policy specification, the code group collection including one or more code groups;

receiving evidence associated with the code assembly;

evaluating membership of the code assembly in the one or more code groups, based on the evidence;

generating the permission set based on the membership of the code assembly in the one or more code groups;

receiving the permission set including at least one permission associated with the code assembly;

receiving a permission request set in association with the code assembly; and

computing a logical set operation on the permission set and the permission request set to generate a permission grant set.

36. The computer program product of claim 35 wherein the permission request set includes an optional request set specifying an optional set of permissions requested in association with the code assembly and a minimum request set specifying a minimum set of permissions requested in association with the code assembly, and wherein the filtering operation comprises:

computing a union of the optional request set and minimum request set to provide a maximum request set; and

computing an intersection of the maximum request set and the permission set.

37. The computer program of claim 36 wherein the permission request set further specifies a refuse request set specifying a set of one or more permissions to be omitted from a permission grant set in associated with the code assembly, and wherein the filtering operation further comprises:

subtracting the set of one or more permissions specified in the refuse request set from the intersection of the maximum request set and the permission set.